

Anmol Yadav

+91-9580550791 | Pune, Maharashtra | work.anmolyadav@gmail.com | [LinkedIn](#) | [GitHub](#) | [Portfolio](#)

SUMMARY

Final-year Computer Science undergraduate specializing in **AI, Backend** and **Cybersecurity**, with hands-on experience building agentic LLM pipelines and autonomous security assessment tools. Backed by a strong offensive security background, including **25+ disclosed vulnerabilities** and a global CTF ranking, and active open-source contributions.

PROJECTS

- Recon AI: Autonomous Attack Surface Assessment** | *Python, LangGraph, FastAPI, RAG* [Demo](#) | [GitHub](#)
- Engineered an agentic orchestration pipeline using LangGraph and FastAPI, coordinating 3 specialized LLM components (Planner, Analyst, Reporter)
 - Built a concurrent subprocess engine orchestrating **30+ security tools** across sequential recon stages, executing independent tools in parallel and aggregating their outputs into a local **RAG** pipeline
 - Designed a dependency-aware execution pipeline that **propagates and normalizes outputs** across **recon stages**, enabling discovered subdomains and live hosts to dynamically drive downstream scans
 - Developed a React frontend utilizing **FastAPI WebSockets** with custom replay buffers for live 0–100% progress streaming, featuring interactive metrics modals with **3 one-click export formats** (JSON, CSV, TXT).
- Multi-Tenant Cloud IDE** | *React, Node.js, Docker, WebSockets, AWS, Prometheus, Grafana* [Live](#) | [GitHub](#)
- Architected a **full-stack Cloud IDE** provisioning isolated, resource-capped Docker containers per user — supporting **5 concurrent** multi-tenant sandboxed environments with semaphore-enforced pool limits
 - Built a **real-time bash terminal** using **node-pty** and **xterm.js** over WebSockets (Socket.io) for a seamless in-browser coding experience
 - Instrumented a **Prometheus + Grafana** observability stack for real-time monitoring of active containers
 - Hardened container isolation by running each sandbox with a non-root user, dropped Linux capabilities, and read-only root filesystem where possible, reducing the attack surface of untrusted user-submitted code execution

EXPERIENCE & LEADERSHIP

- Co-Head & Tech Lead** Aug. 2025 - May 2026
Localhost, Dev Club of IIIT Pune Pune, Maharashtra
- Coordinated Nexus 2.0, a 24-hour offline hackathon - screened 1000+ registrations on Hack2Skills and shortlisted 40+ teams; oversaw end-to-end event execution and quality validation pipeline
 - Developed and maintained the official club website, shipping new features and resolving production bugs to improve performance and UX for 1000+ student users
- Placement Coordinator** Mar. 2025 - Present
Training & Placement Cell, IIIT Pune Pune, Maharashtra
- Part of the core team coordinating offline placement drives with **30+ companies** — handled scheduling, venue coordination, and on-ground logistics

ACHIEVEMENTS

- Identified and responsibly disclosed **25+** web application **vulnerabilities** affecting production systems, resulting in remediation by impacted organizations.
- Achieved **global Rank 80 out of 2,000+** participating teams in **Apoorv CTF 2026**, solving complex cybersecurity challenges spanning web exploitation, forensics, and cryptography.
- Open Source Contributor – AsyncAPI Initiative**: Improved UI consistency and cleaned configuration files through 3 merged pull requests.
- Ranked in the **Top 3% globally** on TryHackMe among **8M+ users**, demonstrating strong hands-on experience across practical cybersecurity challenges and security assessment labs.
- Secured **1st place** in a hackathon organized by Quine among **100+ teams** (2023), competing against teams to design and implement a solution under time constraints.

TECHNICAL SKILLS

Languages : Python, JavaScript, C/C++
Backend & APIs: Node.js, FastAPI, REST APIs, SQL, WebSockets, Redis, MongoDB
AI & LLM: LangGraph, LangChain, LLM Integration, RAG, AI Security
Cloud & DevOps: AWS, Docker, Nginx, GitHub Actions, Prometheus, Grafana
Security: Network Security Testing, API Testing, Vulnerability Assessment, OWASP Top 10, Burp Suite, Kali Linux
Frontend: React.js, Next.js, Redux Toolkit, Tailwind CSS, xterm.js, Socket.io
Core CS: Data Structures & Algorithms, Object-Oriented Programming, Operating Systems, Computer Networks, DBMS

EDUCATION

Indian Institute Of Information Technology, Pune Pune, Maharashtra
Bachelor of Technology in Computer Science Aug. 2023 - May 2027

CERTIFICATIONS

Jr Penetration Tester — TryHackMe May 2025
Web Fundamentals — TryHackMe Apr. 2025